



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,860	05/22/2001	Mark Joseph Stefan Jarosz	190-1477	1072

7590 09/30/2004

William M. Lee, Jr.  
Lee, Mann, Smith, McWilliams, Sweeney & Ohlson  
P.O. Box 2786  
Chicago, IL 60690-2786

EXAMINER

ADAMS, JONATHAN R

ART UNIT PAPER NUMBER

2134

DATE MAILED: 09/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/862,860	<b>Applicant(s)</b> JAROSZ, MARK JOSEPH STEFAN	
	<b>Examiner</b> Jonathan R Adams	<b>Art Unit</b> 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 22 May 2001.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☐ Claim(s) \_\_\_\_\_ is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### ***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1, 9 rejected under 35 U.S.C. 103(a) as being unpatentable over Brown et al., US Patent No 6732179 (hereafter referred to as '179) in view of Oehrke et al., US Patent No 6735631 (hereafter referred to as '631).

As to claim(s) 1, 9:

3. '179 teaches a computer system providing secure connections between a first node and a plurality of third load balanced nodes using authentication and shared secrets comprising:

- First node connected to second node and plurality of third nodes / Client (First node) communicates with servers (Third nodes) (Col 7, Line 15, '179) Walled garden proxy server (second node) (Col 2, Line 53, '179)
- Communication between first node and third node is encrypted / client communicates with servers using SSL (Col 7, Line 15, '179)

Art Unit: 2134

- Selecting a third node and setting upon encrypted connection / A single service can reside on multiple servers such as when load balancing is being employed (Col 9, Line 42, '179)
- First node and plurality of third nodes form a virtual private network / CMTS allows client to access a private network (Col 2, Line 53, '179). Servers coupled to the walled garden network in virtual private network (Col 2, Line 64, '179)
- Communications encrypted with message encryption key established after an authentication process / Client authentication, Encrypted SSL connection using shared secrets (message encryption key) (Page 2, Lines 6-18 and 27, Intro to SSL)
- Key management service selects third node and attempts to perform authentication / Client sends settings to the selected server (Page 6, Line 32, Introduction to SSL)
- After authentication, message encryption key is stored at first and third nodes / client and server use session keys to encrypt transmission data (Page 7, Line 28, Introduction to SSL)

4. '179 does not specifically teach detecting failure of the selected third node. '631 teaches a load balancing system for detecting errors and redirecting users to alternate redundant servers (Col 4, Line 1 et seq., '631). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the error detection/redirection load balancing strategy listed in '631 with the load balanced redundant servers listed in '179. One of ordinary skill in the art would have been motivated to use the error

Art Unit: 2134

detection/redirection load balancing strategy listed in '631 with the load balanced redundant servers listed in '179 because it is beneficial to users that they receive no perceivable loss in services.

5. Claims 2-7 and 10-13 rejected under 35 U.S.C. 103(a) as being unpatentable over '179 in view of '631 in further view of Allison et al., US Patent No 5917900 (hereafter referred to as '900).

As to claim(s) 2:

6. '179 as modified above teaches a computer communications system providing secure connections between a first node and a plurality of third load balanced nodes using authentication and shared secrets. '179 as modified above does not specifically teach for the communications system which also manages keys to randomly select the third node from the plurality. '900 teaches the load balancing strategy of random selection of servers (Col 1, Line 33, '900). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the random selection load balancing strategy of '900 during normal unfailing operation of the servers in '179. One of ordinary skill in the art would have been motivated to use the random selection load balancing strategy of '900 during normal unfailing operation of the servers in '179 because random selection guarantees an average equal distribution between servers reducing the load on any given server, which could otherwise lead to slowed or failed server operations.

7. As to claim(s) 10:

Claim 10 further comprises:

Request for a message key / Generating a message encryption key for first and third nodes / client and server use session keys to encrypt transmission data (Page 7, Line 28, Introduction to SSL)

Performing an authentication process with selected third node / Client authentication, Encrypted SSL connection using shared secrets (message encryption key) (Page 2, Lines 6-18 and 27, Intro to SSL)

8. As to claim(s) 3:

First node and respective third nodes includes respective IP filter [connection protocol selected packet flow] which detects third node failure / IP filter of the first node sends failure detection signal [SSL communication in TCP/IP with expected response] to third node / IP filter of third node sends a response if operational / due to cached IP addresses, if the server becomes unavailable, the user experiences outages [of unreturned outbound queries from server filtering all inbound packets] (Col 2, Line 16, '631)

If no response, first node selects other third node with other message encryption key / If no third node key is available another key is generated from key management service / A single service can reside on multiple servers such as when load balancing is being employed (Col 9, Line 42, 179) with new SSL connection and generated session key

9. As to claim(s) 4, 11:

Failure detection signal is transmitted with a respective message encryption key has been established and no communication from selected third party has been received within a predetermined time interval / any unreturned queries sent after an SSL connection is established can be considered failure detection signals. TCP as standard used on the Internet with SSL uses several timeout functions (See Pages 297-300, TCP/IP Illustrated)

10. As to claim(s) 5, 12:

When message encryption keys have been established for more than one third node, failure detection signal is only sent to selected third node / If multiple SSL server connection instances exist on first node a query only detects failure when third node does not respond

11. As to claim(s) 6, 7, 13:

Transmission of failure detection signal [SSL communication in TCP/IP with expected response] is deferred until after the first node has transmitted encrypted communications to the selected third node / Failure detection signal is encapsulated in communications / failure detection signal [SSL communication in TCP/IP with expected response] can only exist after encrypted SSL communications have begun

Art Unit: 2134

12. Claim 8 rejected under 35 U.S.C. 103(a) as being unpatentable over '179 in view of '631 in further view of '900 in further view of "Undernet IRC Servers" (hereafter referred to as MIRC).

As to claim(s) 8:

13. '179 as modified above teaches a computer system providing secure connections between a first node and a plurality of third load balanced nodes using authentication and shared secrets. '179 as modified above does not teach the use of randomly selecting a server from a list of potential servers stored in a file on the first node. MIRC teaches the use of randomly selecting a server from a list of potential servers stored in a file on the first node (Page 1, Line 2 and 19, MIRC). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the system of random server selection from a file as done in MIRC with the invention of '179 as modified above. One of ordinary skill in the art would have been motivated to use the system of random server selection from a file as done in MIRC with the invention of '179 as modified above because this mechanism works as an additional load balancing system speed server client interactions.

### **Conclusion**

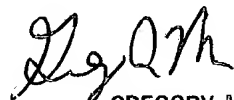
14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is



Art Unit: 2134

(571)272-3832 after 10/04. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

15. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100